



# **COMPLIANCE AND CONTROL AUDIT REPORT**

**Kansas Department of Health and Environment  
Information Systems: Reviewing the  
Department's Management of Those Systems**

**A Report to the Legislative Post Audit Committee  
By the Legislative Division of Post Audit  
State of Kansas  
October 2003**

# ***Legislative Post Audit Committee***

---

## ***Legislative Division of Post Audit***

**The Legislative Post** Audit Committee and its audit agency, the Legislative Division of Post Audit, are the audit arm of Kansas government. The programs and activities of State government now cost about \$9 billion a year. As legislators and administrators try increasingly to allocate tax dollars effectively and make government work more efficiently, they need information to evaluate the work of government agencies. The audit work performed by Legislative Post Audit helps provide that information.

We conduct our audit work in accordance with applicable government auditing standards set forth by the U. S. General Accounting Office. These standards pertain to the auditor's professional qualifications, the quality of the audit work, and the characteristics of professional and meaningful reports. These audit standards have been endorsed by the American Institute of Certified Public Accountants and adopted by the Legislative Post Audit Committee.

The Legislative Post Audit Committee is a bipartisan committee comprising five senators and five representatives. Of the Senate members, three are appointed by the President of the Senate and two are appointed by the Senate Minority Leader. Of the representatives, three are appointed by the Speaker of the House and two are appointed by the House Minority Leader.

As part of its audit responsibilities, the Division is charged with meeting the requirements of the Legislative Post Audit Act which address audits of financial matters. Those requirements call for two major types of audit work.

First, the Act requires an annual audit of the State's financial statements. Those statements, prepared by the Department of Administration's Division of Accounts and Reports, are audited by a certified public accounting firm under contract with the Legislative Division of Post Audit. The firm is selected by the Contract Audit Committee, which comprises three members of the Legislative Post Audit Committee (including the Chairman and Vice-

Chairman), the Secretary of Administration, and the Legislative Post Auditor. This audit work also meets the State's audit responsibilities under the federal Single Audit Act.

Second, the Act provides for a regular audit presence in every State agency by requiring that audit work be conducted at each agency at least once every three years. Audit work done in addition to the annual financial statement audit focuses on compliance with legal and procedural requirements and on the adequacy of the audited agency's internal control procedures. These compliance and control audits are conducted by the Division's staff under the direction of the Legislative Post Audit Committee.

### **LEGISLATIVE POST AUDIT COMMITTEE**

Representative John Edmonds, Chair  
Representative Tom Burroughs  
Representative Bill McCreary  
Representative Frank Miller  
Representative Dan Thimesch

Senator Derek Schmidt, Vice-Chair  
Senator Bill Bunten  
Senator Anthony Hensley  
Senator Dave Kerr  
Senator Chris Steineger

### **LEGISLATIVE DIVISION OF POST AUDIT**

800 SW Jackson  
Suite 1200  
Topeka, Kansas 66612-2212  
Telephone (785) 296-3792  
FAX (785) 296-4482  
E-mail: [LPA@lpa.state.ks.us](mailto:LPA@lpa.state.ks.us)  
Website: <http://kslegislature.org/postaudit>  
Barbara J. Hinton, Legislative Post Auditor

The Legislative Division of Post Audit supports full access to the services of State government for all citizens. Upon request, Legislative Post Audit can provide its audit reports in large print, audio, or other appropriate alternative format to accommodate persons with visual impairments. Persons with hearing or speech disabilities may reach us through the Kansas Relay Center at 1-800-766-3777. Our office hours are 8:00 a.m. to 5:00 p.m., Monday through Friday.



LEGISLATURE OF KANSAS  
**LEGISLATIVE DIVISION OF POST AUDIT**

800 SOUTHWEST JACKSON STREET, SUITE 1200  
TOPEKA, KANSAS 66612-2212  
TELEPHONE (785) 296-3792  
FAX (785) 296-4482  
E-MAIL: [lpa@lpa.state.ks.us](mailto:lpa@lpa.state.ks.us)

October 15, 2003

To: Members, Legislative Post Audit Committee

Representative John Edmonds, Chair  
Representative Tom Burroughs  
Representative Bill McCreary  
Representative Frank Miller  
Representative Dan Thimesch

Senator Derek Schmidt, Vice-Chair  
Senator Bill Bunten  
Senator Anthony Hensley  
Senator Dave Kerr  
Senator Chris Steineger

This report contains the findings, conclusions, and recommendations from our completed performance audit, *The Kansas Department of Health and Environment Information Systems: Reviewing the Department's Management of Those Systems*.

The report includes several recommendations for the Department. We would be happy to discuss these recommendations or any other items in the report with any legislative committees, individual legislators, or other State officials.

Barbara J. Hinton  
Legislative Post Auditor



# EXECUTIVE SUMMARY

LEGISLATIVE DIVISION OF POST AUDIT

## Overview of the Kansas Department of Health and Environment's Information Systems Function

*The Department of Health and Environment is a diverse agency whose mission is to protect and promote the health of Kansans through efficient public health programs and services and through preservation, protection, and remediation of natural resources and the environment.* ..... page 2

*Information systems development and support for the agency is provided by the Information Services Office which is headed by the Director of Information Systems and has a staff of 59 FTE. They support computer operations for the Department's offices in Topeka, the 6 district offices across the State, and multiple county health departments. The Office recently created a security officer position and will eventually have other security positions.*

## Question 1: How Well Is the Kansas Department of Health and Environment Managing the Security of Its Information Systems?

**The Department's operations were at an extremely high risk of fraud, misuse, or disruption.** *KDHE had many of the standard security policies we expected to see, but staff were not following many of the most important policies. Because of the high risk this posed, we met with the Secretary on August 14<sup>th</sup> and made interim recommendations aimed at immediately reducing the risk level. The Secretary and his staff reacted promptly to comply with the recommendations. The extremely high risk was caused largely by the following problems:* ..... page 3

- *KDHE's method of issuing and handling passwords was profoundly flawed, giving any former or current employee—and most hackers—fairly easy access into the agency's network and data. Using password cracking software, we were able to crack more than 1,000 of the agency's passwords (about 60% of the total) in 3 minutes, including several administrative passwords.*
- *The Department's anti-virus system was badly flawed, allowing computers to become infected with a large number of different viruses, worms, and trojan horses. Many computers weren't receiving the necessary virus protection updates, some were set to ignore viruses, and nearly 200 computers didn't have the anti-virus software installed. Many computers were infected with viruses, and some had been infected for months.*

- *The Department's firewall was poorly configured, creating several large holes into and out of the agency.*
- *KDHE had no organized system of tracking user activity. This could prevent the Department from tracking what happened during a security incident.*

*Based on our interim recommendations, KDHE staff addressed each of these areas. These improvements go a long way toward lowering the agency's risk to a more acceptable level.*

**Many other security-related policies were missing, inadequate, or not being followed. Among them were the following:** ..... page 6

- *KDHE had no written procedures related to incident response and reporting.*
- *KDHE wasn't following its policy requiring security to be considered at each stage of a system development project.*
- *KDHE wasn't following its policies on physical security.*
- *KDHE hadn't followed its policy for documenting how its servers were configured.*
- *KDHE wasn't always following its policies to delete the user accounts of employees who leave the agency.*

**The Department could have discovered and resolved these problems using adequate security management planning.** *Without good security planning, there's an increased risk agencies will have weak security over their information systems, or will focus their security resources in the wrong directions. Leading organizations use a cycle of planning activity consisting of analyzing risks, developing policies to address the risks, and monitoring the effectiveness of those policies. Properly used, this cycle provides continuous feedback on the state of security.* ..... page 8

*We found several major problems with the Department's security planning.*

*The IS Department has never done a risk assessment of KDHE's security vulnerabilities. A risk assessment is the base from which all security policies and plans should flow, and allows agencies to identify where their security systems are most vulnerable. It can also help them decide where to focus their limited security resources.*

*The internal committee KDHE formed to develop security policies and procedures and coordinate security failed to complete its job. In 2001, KDHE formed a committee of upper-level managers from all parts of the Department to develop security policies and manage security. Such a group can play an important part in managing security. The Security Council developed a set of policies, but it never followed through to develop procedures or to monitor security. In addition, the policies they developed clearly didn't flow from a risk assessment. KDHE recently made a large step toward improving its security management by creating a position of security officer and hiring a highly qualified person to fill that position.*

*KDHE staff generally weren't monitoring security issues, and didn't use intrusion detection equipment or vulnerability checking software. Information system security involves a complex set of activities that are continually in flux, and that involve a number of people. The only way for upper-level management to ensure that security policies are carried out and remain effective is to monitor those policies and controls. Monitoring can take many forms, such as auditing, reviewing software and hardware configurations, using vulnerability checking software, and regularly reviewing security logs. We found little evidence that active monitoring was occurring. For example, if anyone had checked to see if the weekly anti-virus updates were getting done, or had reviewed the virus logs to see if any machines had become infected, they would have discovered the anti-virus software wasn't working as intended. There also appeared to be some confusion about who was responsible for important security monitoring tasks.*

*KDHE's security policies don't address security awareness. Regular employees are generally considered to be the most significant security risk in any organization. Therefore, it's imperative to educate employees about security and the important role they play in the process. Although the computer support section has undertaken some security awareness activities, no formal classes have been offered on security.*

**Conclusion** ..... page 10

**Recommendations** ..... page 10

## **Question 2: Has the Department Done Adequate Disaster-Recovery Planning To Minimize the Loss of Computer Operations In Case of a Disaster?**

**An organization needs good business continuity planning in order to quickly recover critical operations after a disaster.** ..... page 13  
*Business continuity planning addresses an organization's ability to continue functioning when normal operations are disrupted. By necessity, it includes planning for contingencies and is focused on the information system functions that are the most critical to continue agency operations.*

**KDHE lacks the tools necessary to recover operations quickly after a disaster.** ..... page 13  
*KDHE developed a business-continuity plan for Y2K, but hasn't done any planning since then. The information technology department has a good system for backing-up servers and databases, and has off-site storage of the back-up tapes. However it has no policies relating to disaster recovery planning, and the plan left over from Y2K would be nearly useless in a disaster.*

<b>Recommendations</b>	.....	page 14
<b>APPENDIX A: Scope Statement</b>	.....	page 15
<b>APPENDIX B: Interim Recommendations</b>	.....	page 17
<b>APPENDIX C: Agency Response</b>	.....	page 18

This audit was conducted by Allan Foster. If you need any additional information about the audit's findings, please contact Mr. Foster at the Division's offices. Our address is: Legislative Division of Post Audit, 800 SW Jackson Street, Suite 1200, Topeka, Kansas 66612. You also may call us at (785) 296-3792, or contact us via the Internet at [LPA@lpa.state.ks.us](mailto:LPA@lpa.state.ks.us).



# The Kansas Department of Health and Environment Information Systems: Reviewing the Department's Management of Those Systems

---

This is the third in a series of specialized compliance and control audits designed to focus on an important area of agency operations that generally hasn't been reviewed—the technical aspects of operating information systems. At the direction of the Legislative Post Audit Committee, this audit focused on the management of the Department's information systems. Specifically, we reviewed how well the Department secures its information systems. The audit addresses the following questions:

1. **How well is the Kansas Department of Health and Environment managing the security of its information systems?**
2. **Has the Department done adequate disaster-recovery planning to minimize the loss of computer operations in case of a disaster?**

To answer these questions, we reviewed applicable information system standards and best practices in each of the areas listed above, interviewed KDHE officials, reviewed and evaluated policies and other documentation, and tested selected computer controls used by KDHE in managing its computer systems.

A copy of the scope statement for this audit approved by the Legislative Post Audit Committee is included in Appendix A. For reporting purposes, we've expanded the scope statement's one question into 2.

The criteria we used in reviewing the Department's management efforts came from 2 main sources:

- the Control Objectives for Information and Related Technology (COBIT), published by the Information Systems Audit and Control Association
- the Federal Information System Controls Audit Manual, published by the U.S. General Accounting Office.

In conducting this audit, we followed all applicable government auditing standards. Our findings begin on page 3, following a brief overview.

## Overview of the Kansas Department of Health and Environment's Information Systems Function

---

The Department of Health and Environment (KDHE) is a diverse agency whose mission is to protect and promote the health of Kansans through efficient public health programs and services, and through the preservation, protection, and remediation of natural resources and the environment.

---

### ***KDHE's Office of Information Services Is Responsible for Computer Operations And Security***

This office is located within the Administrative program, and is headed by the Director of Information Systems. It has a staff of 59 FTE positions, 6 of which are currently vacant.

The office is responsible for coordinating the collection, storage, processing, and dissemination of data for KDHE. It also provides support and training on computerized systems and programs to KDHE staff, including the Department's offices in Topeka, the 6 district offices across the State, and multiple county health departments. The director reports directly to the Secretary.

The office of Information Services historically has had 3 main sections:

- Computer Support—18 staff support the desktop computers and provide computer training
- Database/Applications—21 staff create and maintain applications and databases
- Networking Services—10 staff support the network and servers

In addition, a newly created section for Security and Network Infrastructure eventually will have a staff of 5 to handle security and various aspects of the network.

**Information Services supports the operational bureaus through a large number of computerized applications, many of which house critical sensitive data.** Among the most sensitive applications are those dealing with:

- vital statistics—contains data on births, deaths, marriages, and divorces
- health services for children—contains information on children with special health needs and the services provided to them
- child care licensing—contains information on child care facilities such as background checks, applications, inspections, complaints, and enforcement tracking
- children and families—tracks services provided to clients by county health departments for various programs
- epidemiology—has a database of disease-tracking information from public health providers

## Question 1: How Well Is the Kansas Department of Health and Environment Managing the Security of Its Information Systems?

---

KDHE has adopted many of the necessary policies related to information systems security, but its staff generally haven't followed those policies. As a result, the Department's operations were at a very high risk of fraud, misuse, or disruption. In addition, the Department's data were at an equally high risk of loss or inappropriate disclosure. Some of the problems identified: KDHE was ignoring its password policies and using a fundamentally flawed method of handling passwords. It had misconfigured its anti-virus software, allowing infections of serious viruses to be ignored. And its firewall allowed unneeded access to the network. The Department's policies were inadequate or ignored in several other areas as well. It appeared that a lack of organized security planning allowed the Department's problems to develop and go uncorrected. These and other findings are discussed in the sections that follow.

---

### ***The Department's Operations Were At an Extremely High Risk of Fraud, Misuse, or Disruption***

Today, information technology is becoming more and more imbedded in business strategies and operations. Likewise, technology is increasingly being used to make services more efficient and effective for the public and for State agencies. As a result, keeping information systems and the data in them secure has become an essential function.

Security policies are the core of an organization's security efforts. When we compared KDHE's written security policies against standard best practices, we noted that KDHE had developed 48 of the 58 security-related policies we had expected to see. There were no policies in 10 other areas, including those related to risk and vulnerability assessments, business continuity planning, and server configuration management.

Of the 48 policies KDHE had developed, we concluded that 4 were inadequate. Further, our tests of 20 of these established policies showed that KDHE staff were following only 5 (25%), were partially carrying out 4 more, and weren't following the remaining 11. Because the Department's data systems were at significant risk of fraud, misuse, or disruption, we concluded KDHE needed to take immediate action to protect itself and its data.

To address these risks, we met with the Secretary on August 14 and outlined a series of immediate actions needed to address them. (These recommendations are included as Appendix B of the report.) The Secretary and his staff responded promptly to resolve the issues we had identified. Because those security-related issues were resolved, we are able to discuss them freely in the following sections. Other findings are reported in more general terms.

**KDHE's method of issuing and handling passwords was profoundly flawed, giving any former or current employee—and most hackers—fairly easy access into the agency's network and data.** Passwords are the most commonly used method for controlling access to computer systems, but they are also the weakest form of access control. As a result, it's important to have good password controls and to rigorously enforce those controls, especially for an agency that has as much confidential data as KDHE.

KDHE had established policies related to password controls that addressed most of the standard recommended security procedures. However, we found that it wasn't following any of them. For example:

- employees were issued passwords using one of two simple, easy to guess patterns
- users weren't required to change their passwords on a periodic basis; in fact, most user accounts were set to not allow users to change their passwords
- none of the network password settings were enabled (in other words, no password controls were being used on the network)
- no limits were set on the number of unsuccessful password guesses allowed before the account was locked

Using standard password cracking software, we were able to crack more than 1,000 of the agency's passwords (about 60% of the total) in 3 minutes. Within 11 hours, we had cracked 90% of its passwords. The most important passwords are those of the network administrators. These passwords can access just about anything and give the user nearly unlimited power on the network. We cracked 15 of 21 administrative passwords in our test, including 4 within 2 minutes.

Given the simple pattern to KDHE's assigned passwords and the absence of any of the standard security controls, current or former employees would have been able to log onto most KDHE employees' computers within just 2 attempts. Any actions taken while logged onto that employee's computer would appear to have been made by the employee, not by the intruder. This weakness put the entire network and all agency data at severe risk.

**The Department's anti-virus system was badly flawed, allowing computers to become infected with a large number of different viruses, worms, and trojan horses.** Although KDHE's policies on virus control generally were adequate, we found that those policies weren't always followed. When the Department's new security officer checked the software in early August, she found that it wasn't set up correctly. Four major things were wrong:

- the system the software uses to distribute the patterns used to identify new viruses to servers and computers was misconfigured, preventing many computers from receiving the necessary virus protection updates
- on many computers, the software was set to ignore viruses
- nearly 200 computers didn't have anti-virus software installed
- the software was logging the infections that occurred, but no one was looking at the logs

The security officer found that at least 30 computers were infected with 16 different viruses, worms, and trojan horses. Although a few of the viruses were fairly harmless, 16 computers had viruses or trojan horses that could send files and passwords from the computers to addresses outside the agency.

In addition, 2 of the viruses could install programs that record all keystrokes made on the computer. (There's no way to tell if any data actually were sent outside the agency.) Some computers had multiple cases of these viruses, some had been infected for months, and one computer had a list of infected files more than 9 pages long.

#### **The Department Supplemented Our Audit Work With a More Technical Review by a Consulting Firm**

In response to one of the recommendations we made on August 14<sup>th</sup>, the Department contracted with Fishnet Securities, a large midwestern network security consulting firm, to do an in-depth vulnerability assessment audit. Because of the severity of the higher-level problems we identified, we thought it important for the Department to identify the depth of its technical problems. In late August, Fishnet conducted tests of:

**physical security controls**—a Fishnet employee tested physical controls by wandering around the Department's offices in Topeka picking up files and laptop computers from various offices.

**external network vulnerabilities**—Fishnet used vulnerability checking software to scan various servers and workstations on the network that are accessible from the Internet to identify areas where the machines were vulnerable to attack from outside the network.

**application vulnerabilities**—Fishnet used software designed to check computer applications for vulnerabilities. Vulnerabilities in applications are ignored by most security scans, but are becoming significant areas of risk for organizations. This is especially true for web-based applications. These vulnerabilities are often harder to address than network-level vulnerabilities.

**wireless network vulnerabilities**—These tests monitored for vulnerabilities in wireless applications, and tested for rogue wireless equipment (wireless equipment hooked to the network that wasn't authorized by the Department).

In their final report, Fishnet identified a number of vulnerabilities that the Department is beginning to address.

**The Department's firewall was poorly configured, creating several large holes into and out of the agency.** Firewalls create protected borders between the Internet and the agency's internal network, or between different portions of a network. In order to communicate with the outside world, small openings are created in the firewall to let particular groups of people in or out to do particular things. Some openings need to be large—such as letting anybody who's inside the network out to browse the Internet. Other openings may be very small—such as allowing a particular computer in to do one particular thing.

We noted that the openings in KDHE's firewall granted far more access than was necessary or prudent. For example, the firewall:

- opened the entire internal network to the Department of Administration's Division of Information Systems and Computing
- opened internal servers housing sensitive databases to the "demilitarized zone" (the less-secure portion of the network between the public Internet and the highly protected internal network)
- put one server completely outside the firewall, leaving it unprotected from hackers

**KDHE had no organized system of tracking user activity.** Audit trails within computer systems provide accountability. They allow staff to track important actions—such as successful and unsuccessful log-in attempts, changes to access privileges, and files that have been accessed. Without such logs, it's nearly impossible to track what happened during a security incident.

KDHE had developed adequate policies in this area, but we found that security logs had not been turned on for some servers, that there were no logs on any of the desktop computers, and that no one periodically monitored the activity reported on the logs that did exist.

---

***Many Other Security-Related Policies Were Missing, Inadequate, or Not Being Followed***

The problems we identified are summarized below:

- KDHE had no written procedures related to incident response and reporting. Such procedures establish guidelines for how staff are to respond to various types of security incidents. They are important so that staff will know what to do in case of a serious security incident (such as cutting off an intrusion immediately, or tracking the intruder long enough to collect the information needed to prosecute the attacker), and who is to do it. Speed is also essential in responding to such an attack in order to protect agency data. We also noted that the general policies in this area made operational bureaus within KDHE responsible for investigating security incidents. Such investigations should be the responsibility of the IS department.



- KDHE wasn't following its policy requiring security to be considered at each stage of a system development project. System development literature shows that security is often added at the end of a software development project, or after a project has been completed. Building in security early in the project results in more secure systems and costs far less. Best practices call for security plans to be developed for all projects under development, and for each phase of system development to include assurances of security and audit controls. KDHE had such a policy, but hadn't implemented it.
- KDHE wasn't following its policies on physical security. During one lunch hour, our staff and KDHE's new security officer were able to enter empty offices on 3 different floors to check the computers, and were only questioned by one person. Many computers were logged onto the network and unlocked. We also found an unlocked wiring closet, and noted that the area where new computers were setup was unlocked and unoccupied.
- KDHE has no policies or procedures on network banner language. A network banner is a welcoming screen that comes up when someone starts to log onto a computer. Its purpose is to provide notice of legal rights to users of the network. They generate consent for administrators to monitor activity and to retrieve files and records. Without such banners, KDHE might have trouble prosecuting hackers or monitoring the network for unauthorized activity. KDHE has been considering some banner language for some time, but hasn't adopted it.
- KDHE didn't have a policy for documenting how its servers were configured. Such documentation is important to ensure that any servers that have to be replaced or rebuilt are configured correctly and securely. Mistakes in configuration can often open a server to a hacker.
- KDHE wasn't always following its policies to delete the user accounts of employees who leave the agency. We checked the accounts of 35 employees who had left KDHE in the past year and found about a third to still be active. Leaving these accounts active allows non-employees to have access to the network and files.
- KDHE wasn't following its policies on protecting sensitive agency data on laptops. Possible ways to protect such data: keeping it on diskettes or other removable media, encrypting the documents, and using cable locks to physically secure the laptops.
- KDHE had no policy for ensuring that its security staff get continuing education on an ongoing basis. In addition, officials reported that none of the programmers developing new applications had been provided any security training. Training is especially important for programmers developing web-based applications.

***The Department Could Have Discovered and Resolved These Problems Using Adequate Security Management Planning***

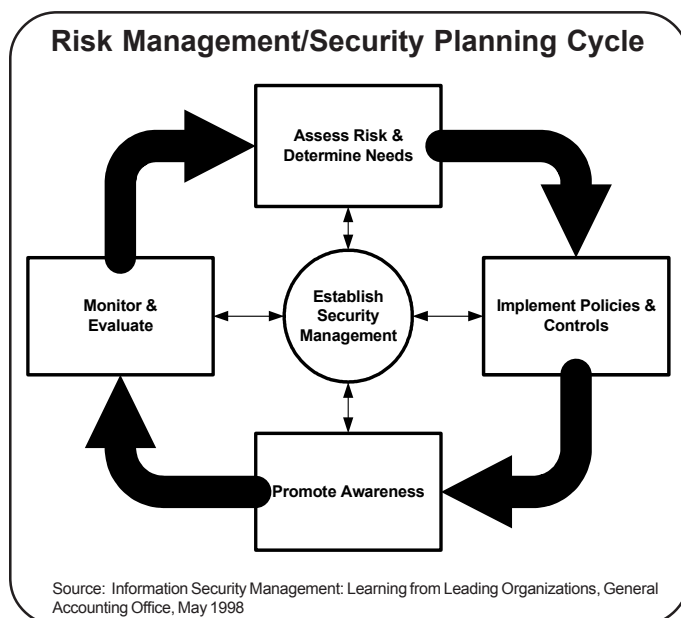
Without good security planning, there's an increased risk agencies will have poor security over their information systems, or will focus their security resources in the wrong directions. Security planning should be an on-going cycle of activity. A U.S. General Accounting Office study of the leading non-federal organizations with the most successful security-management functions found that these organizations use 5 common risk-management principles:

- periodically assess risks
- establish a security-management structure, and clearly assign security responsibilities
- document an entity-wide security plan
- promote security awareness
- monitor the security program's effectiveness, and make changes as needed

These principles form a cycle of activity that can help organizations ensure their security policies are current and address risks on an ongoing basis. As staff go through the cycle, they receive feedback on how well risks are being mitigated, and whether there are risks that are being missed. Weaknesses in how the system is working are continuously pointed out.

We compared the Department's security management processes and practices with this list of critical elements. Our findings are summarized in the following sections.

**The Information Systems (IS) office has never done a risk assessment of KDHE's security vulnerabilities.** The IS director told us the operational bureaus do informal risk assessment as



applications are being developed. However, this is only a small part of what is needed. A risk assessment is the base from which all security policies and plans should flow, and allows agencies to identify where their security systems are most vulnerable. It can also help them decide where to focus their limited security resources.

**The internal committee KDHE formed to develop security policies and procedures and coordinate security failed to complete its job.** In 2001, KDHE formed a committee of upper-level managers from all parts of the Department to develop security policies and manage



security. The Security Council, as it was called, was chaired by the IS director. Designating a central group to handle security is an important element in the planning process.

The Council developed a set of policies, but as described earlier, many of them didn't address some important entity-wide security issues. In addition, those policies clearly don't flow from an assessment of risks. For example, the agency has been working on establishing more web-based applications for epidemiology, vital statistics, and child care licensing. However, no policies or procedures have been developed to address the greater risks of such applications which arise from being so much more exposed to the internet.

We also noted that the Council never followed through on its other responsibilities--to develop procedures and to monitor security. The IS director told us he didn't reconvene the Council because of a lack of time.

KDHE's recent decision to create a security officer position and hire a highly qualified person to fill that position will go a long way towards improving security management. The IS director told us the security officer would chair of the Security Council, which will begin meeting soon to reevaluate the security policies and to carry out its other responsibilities.

**KDHE staff generally weren't monitoring security issues, and didn't use intrusion detection equipment or vulnerability checking software.** Information system security involves a complex set of activities that are continually in flux, and that involve a number of people. Even under the best of circumstances, it's difficult to maintain security at an acceptably high level. The only way for upper-level management to ensure that security policies are carried out and remain effective is to monitor those policies and controls. Monitoring can take many forms, such as auditing, reviewing software and hardware configurations, using vulnerability checking software and other network utilities, regularly reviewing security logs, and conducting self-assessments.

We found little evidence that active monitoring was occurring. For example, if anyone had checked to see if the weekly anti-virus updates were getting done, or had reviewed the virus logs to see if any machines had become infected, they would have discovered the anti-virus software wasn't working as intended. The network manager also told us that when something suspicious happened, he would consult the security logs to investigate. However, the logging function wasn't even turned on for many KDHE servers, and none of the employees'

computers had it enabled. As a result, if an intrusion was discovered, it would be hard to investigate unless it happened on one of the servers with logging enabled. In addition, the network manager apparently had a basic misunderstanding of the security policies and of his staff's role. The policies give important roles to "data custodians" including several monitoring responsibilities. The IS director told us that the IS office was the data custodians, but the network manager thought that the operational divisions of the agency were the custodians.

**KDHE's security policies don't address security awareness.**

Regular employees are generally considered to be the most significant security risk in any organization. Therefore, it's imperative to educate employees about security and the important role they play in the process. Although the computer support section has undertaken some security awareness activities, mainly focusing on viruses and passwords, no formal classes have been offered on security. (Ironically, at the same time the support staff were asking people to change their passwords, the network staff were setting accounts to not allow users to change passwords.)

<b>Conclusion</b>	Before this audit, the Department's computer systems were at an extremely high risk of fraud, misuse, or disruption, and its computer data—much of it confidential—was at an equally high risk of loss or inappropriate disclosure. This situation developed over time through a combination of factors, but the main cause appears to have been a fundamental lack of understanding of computer security by key staff who were charged with that responsibility, and a failure to recognize or act on problems that existed. The Department has acted strongly and swiftly to address these problems—including hiring a respected consulting firm to identify the depth of its technical problems. By taking these actions, the Department has already started lowering the high level of risk that existed at the start of the audit. By implementing the additional recommendations made in this audit and the consultant's report, and by continuing to focus on its critical computer security needs, the Department should be able to overcome these problems and put a security program in place that identifies and mitigates risks before they are realized.
-------------------	---

- |                        |  |
|------------------------|--|
| <b>Recommendations</b> | <ol style="list-style-type: none"><li>1. To ensure that it manages the security of its systems effectively and efficiently, KDHE should adopt a system of security planning similar to the one described in this report. As a part of that process, KDHE should:<ol style="list-style-type: none"><li>a. reinstitute the Security Council with the security officer as the chair</li></ol></li></ol> |
|------------------------|--|

- b. have the Information Systems Office conduct an annual agency wide risk assessment with participation of staff from the operational bureaus
  - c. have the Security Council use the results of the risk assessment to evaluate and update the security policies annually
  - d. have the security officer develop a security monitoring procedure to help ensure that security policies and controls address risk areas effectively, and that staff comply with the policies
  - e. evaluate IS staff job descriptions and insert security duties in those job descriptions where appropriate
2. In evaluating the security policies, the KDHE Security Council should consider developing the following written policies or procedures:
- a. a risk management policy requiring periodic risk assessments designed to identify what the Department's major risks are, and where security controls are needed to mitigate those risks
  - b. incident response and reporting procedures that establish guidelines for how staff are to respond to security incidents. It should also form an incident response team of both IS and operational staff to carry out the procedures.
  - c. an accountability policy specifying what types of audit trails are to be maintained, how long they are to be maintained, and a more detailed requirement on the periodic review of logs
  - d. a configuration management procedure for servers and workstations. It should also adopt a standard for securely configuring different types of equipment.
  - e. a continuing education policy for security staff and programmers to help ensure that staff keep up-to-date on security issues
  - f. a security awareness program for KDHE staff
  - g. a policy requiring servers and computers to be kept current on security patches
  - h. a policy requiring that a network banner be displayed on each computer upon login that meets legal requirements for warning away unauthorized users, and for notifying legitimate users of privacy restrictions and network monitoring
- 3 The Information Systems director should ensure that his staff follow existing policies and procedures, including the policies that require:
- a. password controls to be used
  - b. periodic auditing and monitoring of security
  - c. employee computer accounts to be disabled or deleted when an employee leaves the agency

- d. screen saver passwords to be enabled
  - e. laptops to be stored securely
  - f. sensitive data on laptop computers to be encrypted
  - g. security to be considered during each phase of software development projects
4. To avoid further problems developing because of a lack of communication, the Information System director should ensure that the different sections within the IS Office become less isolated and communicate more effectively.
5. Before the start of the 2004 legislative session, the Department should provide Legislative Post Audit with a corrective action plan for addressing these recommendations and those made by the consulting firm. The plan should prioritize the problems and specify a time schedule for addressing them.

## Question 2: Has the Department Done Adequate Disaster-Recovery Planning To Minimize the Loss of Computer Operations in Case of a Disaster?

---

Business continuity planning addresses an organization's ability to continue functioning when normal operations are disrupted. KDHE hasn't done any business-continuity planning since 1999, increasing the risk it won't be able to respond in the event of a disaster.

---

### ***An Organization Needs Good Business Continuity Planning In Order To Quickly Recover Critical Operations After a Disaster***

Business continuity planning addresses an organization's ability to continue functioning when normal operations are disrupted. By necessity, it includes planning for contingencies and is focused on the information system functions that are the most critical to continue agency operations. Often this is called disaster-recovery planning.

Good business continuity planning involves the following:

- developing a written continuity plan that is in line with the agency's objectives
- testing the plan and keeping it up-to-date
- making sure each employee knows their responsibilities as specified in the plan
- establishing adequate off-site storage for critical backup tapes
- developing alternative processing procedures for user departments to implement until processing can be restored

The continuity plan itself discusses the most likely types of disasters and specifies detailed steps to take to recover services, including assigning specific roles and responsibilities to specific staff members.

---

### ***KDHE Lacks the Tools Necessary To Recover Operations Quickly After a Disaster***

KDHE developed a business-continuity plan for Y2K, but hasn't updated that plan or done any other continuity planning since 1999. We found that the IS office does have a good system for backing-up servers and databases, and has off-site storage of the backup tapes. However, there are no policies concerning business-continuity planning, and the plan left over from Y2K would be nearly useless in an ordinary disaster.

The plan itself does have some good features that would be useful in making a plan. Each business unit in the agency has a section with a concise summary of the work flow as well as manual alternatives to use if computer access isn't available. However, the plan doesn't address the issues that a business continuity plan should address such as:

- possible disaster scenarios with appropriate reactions for each
- roles and responsibilities of specific staff so that people will know what to do

- logistical information on location of key resources such as backup site, applications, data files, and operating manuals
- lists of resources needed to restore operations, such as computers, ancillary equipment, and supplies
- procedures for getting replacement servers and computers ready to load applications and data
- procedures for resuming operations in the original location after the disaster is over

Without an effective plan, the Department's staff would have access to backup data if a disaster affected the central office, but they would have no action plan to let employees know what equipment, software, or supplies they needed to collect, where they should go, or what they should do.

#### **Recommendations**

1. To help ensure that it can continue functioning when normal operations are disrupted by a disaster, KDHE should approve policies requiring it to conduct business continuity planning, which would include the following:
  - a. a risk analysis that assesses the most likely disaster scenarios
  - b. a disaster recovery plan that addresses the disasters most likely to befall the Department. This plan should assign roles and responsibilities to specific staff, and present specific steps for staff to follow in recovering computer operations.
  - c. arrangements that allow KDHE to continue offering computer services in case the central office computers aren't available for a period of time. This could include having redundant servers at an off-site facility, or contracting with a vendor that offers off-site computing capability.
  - d. training staff in how to use the plan in the event of an emergency
  - e. conducting periodic testing of the disaster recovery plan

## **APPENDIX A**

### **Scope Statement**

This appendix contains the scope statement for this audit. This scope statement is being used in a series of compliance and control audits of agency information systems approved by the Legislative Post Audit Committee on December 3, 2001.

## SCOPE STATEMENT

### **Kansas Department of Health and Environment Information Systems: Reviewing the Department's Management of Those Systems**

In fiscal year 2002, the Department of Health and Environment spent about \$6.5 million on its information systems. In all, 52 staff develop and control information systems for the Department. The Department has been re-engineering its information systems, developing new applications, and expanding its accessibility from the internet.

During the last few years, concerns have been expressed about the lack of monitoring of State computer systems. Each year State agencies become more dependent on their computer systems and on the data those systems contain to make decisions and fulfill their missions. More and more, computing is moving out of the data center and into the hands of staff who use the data to make decisions. Computers and computer networks also are being used to communicate with the public, provide services, and conduct business.

These are positive developments that can result in increased efficiency and effectiveness and better service. However, significant risks are associated with these advances in technology that agencies should be addressing and managing. At present there is little oversight of agencies' computer operations to monitor whether these risks are being adequately managed.

To help address these risks, the Legislative Post Audit Committee approved information system audits to be done as an adjunct to the Division's compliance and control audits. This audit looks at the Department's information systems, and will address the following question:

1. **Is the Department of Health and Environment managing its information systems in a manner that reduces the risk of loss due to errors, fraud, or other illegal acts and disasters?** To answer this question, we will review the Department's policies and practices in the following areas:
  - **Security Planning and Management**—We would review the agency's system of managing its information system security, with emphasis on security policies and procedures.
  - **Business Continuity**—We would review the agency's plans for how the staff would continue to operate in situations such as power outages and other disasters, and whether they adequately test those plans. This would include a review of the agency's policies for backing-up computerized data.



## **APPENDIX B**

### **Interim Recommendations**

During the middle of the audit we became concerned about the severity of the security problems we were finding. We decided that several issues warranted immediate attention. Therefore, on August 14, 2003 we discussed our findings with Secretary Bremby and provided him with this list of interim recommendations. The Department has complied with each of the recommendations and satisfactorily resolved the underlying problems.

#### **Kansas Department of Health and Environment Information Systems Interim Recommendations August 14, 2003**

Because of the severity of the problems we have identified, we recommend the agency take the following actions immediately:

1. Enable proper password controls on the network. These should include controls on length of passwords, maximum and minimum password age, use of password history, number of unsuccessful logon attempts, and threshold and duration of account lockout.
2. Require all users to change their network passwords. This should be done without prior notice. Because of the risk that administrative passwords have been compromised, giving notice would allow people to take actions to retain inappropriate access privileges.
3. Contract with an outside consulting firm to do a thorough, technical security audit and vulnerability analysis of the agency focusing on the network. (This audit should include reviewing the firewall rules.) We understand that the security officer has already started the process to contract for some type of security audit. If so, this effort should be expedited.
4. Ensure that the virus protection software is properly configured and tested, and that all viruses have been removed from infected computers.
5. Enable security logging on all servers. This should also be done on all workstations eventually.

## **APPENDIX C**

### **Agency Response**

On October 7, 2003, we provided copies of the draft audit report to the Department of Health and Environment. Its response is included in this appendix.



# K A N S A S

RODERICK L. BREMBY, SECRETARY

DEPARTMENT OF HEALTH AND ENVIRONMENT

October 14, 2003

KATHLEEN SEBELIUS, GOVERNOR

Ms. Barbara Hinton  
Legislative Post Auditor  
Legislative Division of Post Audit  
800 Southwest Jackson Street, Suite 1200  
Topeka, Kansas 6612-2212



Dear Ms. Hinton,

Thank you for the opportunity to review and comment on the draft of the October 2003 Compliance and Control Audit Report of the Kansas Department of Health and Environment's Information Systems.

On behalf of our agency, I would like to express our appreciation for the exemplary overall effort and compliment your staff on their ability to conduct a very thorough and professional audit of this very important agency function. I have reviewed the report and I am in agreement with the findings and recommendations.

The following is the KDHE response to the two questions in that report.

- 1) How well is the Kansas Department of Health and Environment managing the security of its information systems?
- 2) Has the Department done adequate disaster-recovery planning to minimize the loss of computer operations in case of a disaster?

KDHE immediately began addressing the five Legislative Post Audit recommendations with regard to managing the security of its information systems:

1. KDHE is fully committed to maintaining the confidentiality, high availability, and data integrity for all information systems.
  - The KDHE Security Council has been reinstated with the security officer as chair.
2. The KDHE Security Council will develop and implement the recommended policies and procedures.
  - One incident response team has been created. A plan and procedures have been developed and are in draft. Multiple incident response teams and plans will be created.

OFFICE OF THE SECRETARY

CURTIS STATE OFFICE BUILDING, 1000 SW JACKSON ST., STE. 540, TOPEKA, KS 66612-1368

Voice 785-296-0461 Fax 785-368-6368 <http://www.kdhe.state.ks.us>

- A draft configuration for servers has been created. Based on the information found in the consultant's risk and vulnerabilities assessment, a desktop configuration will be created.
  - An appropriate network banner has been implemented.
3. The KDHE Information Systems Director will ensure that IS staff follow existing policies and procedures. Technology will be put into place to automatically enforce adopted procedures, such as enforcing strong passwords and frequent changing of passwords. In addition, KDHE has implemented the following recommendations:
- KDHE has implemented the new password policy, enforced automatically.
  - An outside vendor has completed a vulnerability and risk assessment of the KDHE networks.
  - KDHE will schedule an annual vulnerability and risk assessment.
  - KDHE has implemented the deletion of accounts when employees leave.
  - KDHE will implement screen saver passwords.
  - Software has already been put in place to control access to inappropriate web sites.
4. The KDHE Information System Director will implement processes to improve the communications and working relationships between the Information Technology staffs.
5. KDHE will provide Legislative Post Audit with a corrective action plan for addressing their recommendations and those made by the consulting firm prior to the 2004 legislative session.

With regard to business-continuity, I will ask the Security Council to review and update KDHE's business-continuity plan incorporating the recommendations as outlined in the audit report.

All recommendations will be ranked and prioritized by risk, and deadlines will be established to complete all recommendations as quickly as possible. I encourage a review no later than twelve months from now.

A major key to KDHE's success will be prevention through IT and non-IT employee training. All KDHE employees need to understand that they are not only affected by policies, but they are protected by those same policies. Each employee will be informed that they are personally a part of the KDHE security team, that they are responsible, and do make a difference. Training will be held quarterly to allow each employee the opportunity to learn more about information security and unauthorized access prevention.

Specific training will be provided to IT staff to:

- Create and monitor firewall rules,
- Appropriately review firewall logs frequently,
- Configuring anti-virus software,
- Ensuring the software is updated as timely as possible, and
- System administrator's rights will be restricted to those with the need.

Barbara Hinton  
October 14, 2003  
Page 3

Application programmers and database designers will receive training on:

- The importance of implementing security into their software design,
- The importance of implementing secure database design,
- Secure movement of data from one source to another,
- Applications will be tested on test systems prior to being put into production, and
- Proper use of software change management.


Vendors, through RFP's and maintenance contracts, will be required to:

- Implement security into their applications and databases,
- To implement activity logging as required by KDHE business rules,
- To meet KDHE's internal security requirements, and
- To maintain a current copy of their software on site or in escrow.

I know KDHE will be successful in achieving our objectives and your recommendations.

Again, thank you for the opportunity to comment and clarify information contained in the draft report.

Respectfully,



Roderick L. Bromby  
Secretary